

Remarks

This reply is responsive to the Office communication mailed April 3, 2006. Unless otherwise indicated, page and paragraph references are to that communication.

The independent claims have each been amended to recite that the digital secure repository is accessible to the user "independently of said provider", where the provider is the previously recited entity by whom access rights to the digital content were granted to the user. Support for this new recitation is found in Figs. 8A-8B and the accompanying description, as well as, for example, the statement at page 21, lines 8-10 about the "independence" of the rights wallet authority (108, 128, 204) from the content distribution portal (106, 126, 202).

Claims 1-5, 7-13, 15-17 and 30-31 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Okamoto et al. U.S. Patent 6,732,106 ("Okamoto") in view of Fung et al. U.S. Patent Application Publication 2001/0052077 ("Fung") and newly cited Arima U.S. Patent Application Publication 2002/0035516 ("Arima") (pp. 2-3, ¶ 5). Claims 14 and 18-29 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Okamoto in view of Fung and Arima and further in view of Olson et al. U.S. Patent Application Publication 2002/0003878 ("Olson") (p. 12, ¶ 6). As applied to the claims as amended, this rejection is clearly untenable.

In applicants' claimed invention, a user can render digital content on an authorized rendering device selected from a list of such devices in accordance with the access rights stored in his digital secure repository. The digital secure repository is accessible to the user independently of the content provider so as to allow the user to render the digital content in accordance with such stored access rights without requiring additional authorization from an external authority such as the content provider.

None of the references cited by the Examiner offer this capability individually, nor do they suggest how they might be combined to provide this ability in combination. In Okamoto, as previously recounted, the user is tightly bound, not only to a particular device 1002 (Fig. 2), but also to the distribution server 1001 on which the rights information resides. Similarly, in Fung, a

secret PIN 213 necessary for rendering is stored by the client 102 (¶ 54), in effect binding the digital content to the device of the client 102. This is in addition to the binding created by the UMID 200 itself as a composite of the user ID 210 and device ID 220.

Arima, newly cited by the Examiner, describes a system for user selection (from a user terminal 10) of a “rack” of digital contents for downloading to a player terminal 20 from a content server 30 (Fig. 2). The digital “rack” stored on the server 30 contains a contents storage area and a user information area (¶ 29). As described in paragraph 30 (emphasis added):

A given area in the user information area is allocated to each user ID, and each area includes a password area for saving the password, a player terminal ID area with which a plurality of player terminal IDs can be registered, a link information area for storing link information pointing to locations where digital content products are stored, and a contract information area for storing contract information. The link information area further includes information on the expiration date and the maximum number of replays for each purchased digital contents.

Arima’s player terminal ID area does bear some resemblance to the list 236 of registered rendering devices 206 stored in applicants’ rights wallet 204 (Fig. 2). However, Arima’s system differs critically from applicants’ in that the user information area generally (and thus the portion of the user information area is allocated to particular user ID) is part of the content server 30. Thus, a user’s portion of the user information area is not accessible to the user independently of the content provider, as claimed by applicants.

Arima’s user information area is thus similar to the storage areas of applicants’ content distribution portal 202 (Fig. 2) and Okamoto’s user administration database 1004 (Fig. 4) in that it is not independently accessible by a user, who remains tethered to a content server. Such a user cannot render content on an arbitrarily selected device without the cooperation of the content provider. Indeed, the content server 30 is necessarily involved in protecting the content, since there is no disclosure of how the content is protected once it is transferred from the server 30 to a player terminal 20. This dependence on a central server to manage rendering rights severely

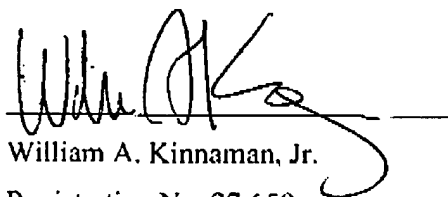
restricts the versatility of the systems described in these references. Applicants avoid these limitations by managing their access rights from an independently accessible digital secure repository, as recited in the claims.

Conclusion

Reconsideration of the application as amended is respectfully requested. It is hoped that upon such consideration, the Examiner will hold all claims allowable and pass the case to issue at an early date. Such action is earnestly solicited.

Respectfully submitted,
GERD BREITER et al.

By



William A. Kinnaman, Jr.

Registration No. 27,650

Phone: (845) 433-1175

Fax: (845) 432-9601

WAK/wak